Claims

We claim:

1. A method comprising the steps of:

transmitting a first packet encrypted using a first encryption vector to a receiving device, wherein the first packet comprises a second encryption vector; and

transmitting a second packet encrypted using the second encryption vector to the receiving device if an acknowledgement message is received within a predetermined period of time after transmitting the first packet; otherwise, re-transmitting the first packet encrypted using the first encryption vector to the receiving device.

2. The method of claim 1 wherein the second packet comprises a third encryption vector.

3. The method of claim 1 and further comprising the steps of:

performing a key exchange with the receiving device to generate a reciprocal set of keys; and

transmitting the first encryption vector to the receiving device.

4. The method of claim 1 wherein the first packet and the second packet comprises physical symbols.

5. The method of claim 4 and further comprising the steps of:

inputting the first encryption vector and a key from the reciprocal set of keys into an encryption engine to generate a first scrambling table for the first packet;

generating an encryption value from the first scrambling table for each physical symbol in the first packet; and

combining each physical symbol in the first packet with an encryption value via an operation in order to encrypt the first packet.

6. The method of claim 5 wherein the operation is one of an exclusive-or operation, a complex multiply operation, a multiply operation, a divide operation, an addition operation, and a subtract operation.

7. The method of claim 5 and further comprising the steps of:

inputting the second encryption vector and the key from the reciprocal set of keys into the encryption engine to generate a second scrambling table for the second packet;

generating an encryption value from the second scrambling table for each physical symbol in the second packet; and

combining each physical symbol in the second packet with an encryption value via an operation in order to encrypt the second packet.

8. A method comprising the steps of:

receiving a first packet from a transmitting device;

decrypting the first packet using a first encryption vector, wherein the first packet comprises a second encryption vector;

transmitting an acknowledgement message for the first packet to the transmitting device;

receiving a second packet from the transmitting device;

attempting to decrypt at least a portion of the second packet using the first encryption vector and the second encryption vector; and

if the at least portion of the second packet was successfully decrypted using the first encryption vector, re-transmitting the acknowledgement message for the first packet; otherwise, transmitting an acknowledgement message for the second packet.

9. The method of claim 8 and further comprising the steps of:

after the step of re-transmitting the acknowledgement message for the first packet, receiving a third packet from the transmitting device; and

attempting to decrypt at least a portion of the third packet using the first encryption vector and the second encryption vector.

10. The method of claim 8 wherein the second packet comprises a third encryption vector.

11. The method of claim 10 and further comprising the steps of:

after the step of transmitting the acknowledgement message for the second packet, receiving a third packet from the transmitting device; and

attempting to decrypt at least a portion of the third packet using the second encryption vector and the third encryption vector.

12. The method of claim 8 and further comprising the steps of:
performing a key exchange with the transmitting device; and
receiving the first encryption vector from the transmitting device.

13. The method of claim 8 wherein the first encryption vector is known *a priori.*

14. The method of claim 8 wherein the step of attempting to decrypt at least a portion of the second packet using the first encryption vector and the second encryption vector is performed concurrently.

15. A receiving device comprising:
carrier sense circuitry,
a first correlator coupled to the carrier sense circuitry;
a second correlator coupled to the carrier sense circuitry;
a processor coupled to the carrier sense circuitry, the first correlator and the second correlator;
a demodulator coupled to the processor, and
a decoder coupled to the processor,
wherein the first correlator, the second correlator, and the processor are in a sleep state until the carrier sense circuitry detects a carrier indicating a transmission of a packet, and wherein the demodulator and the decoder are in a sleep state until at least one of the first and second correlators successfully decrypts a portion of the packet and the processor determines that the packet was not previously transmitted.

16. The receiving device of claim 15 wherein the first correlator and the second correlator decrypts a portion of the packet concurrently.